

## Benefits

### Increase Value from Existing Tools

Consolidate events captured by multiple infrastructure monitoring tools by integrating with them through out-of-the-box connectors, REST API, or SNMP.

### Understand Event Impact on Services

Transform infrastructure events into actionable, service-aware alerts and then see how business services are impacted through a service health dashboard and business service management maps.

### Improve Service Availability

Eliminate service outages by using a range of advanced machine-learning techniques to predict and prevent services outages; integrating with ServiceNow's incident, problem, and change capabilities; and triggering IT processes or automated remediation options.

# ServiceNow Event Management

## The IT Challenge

Enterprises rely on IT to provide the foundation for business services, by maintaining all storage, compute, and network infrastructure. IT may use multiple tools to monitor this infrastructure, but often the high volume of events from these different tools makes it difficult to understand the real issues and take corrective action. Furthermore, there is little visibility into the relationship between infrastructure events and business services, making it difficult to understand which issues should be tackled first. There is no simple, automated way to connect service-impacting events to service management tools and processes for rapid remediation. Because IT cannot monitor the health of business services and infrastructure effectively and respond rapidly to issues that come up, service outages continue to plague the enterprise.

## The ServiceNow Solution

ServiceNow Event Management reduces event noise generated by third-party monitoring tools, uses predictive machine-learning techniques to prevent outages, and creates actionable alerts that enable IT to eliminate service outages. The application brings events captured by existing infrastructure monitoring tools into ServiceNow for consolidation, analysis, and action. Events are then processed through filters that normalize and de-duplicate the incoming event stream to generate alerts, reducing event noise by up to 99%.

When used with ServiceNow Operational Intelligence, Event Management can also generate alerts from infrastructure anomalies that indicate potential service outages. Event Management may also be used with ServiceNow Service Mapping to map alerts to service maps and provide an intuitive service health dashboard, enriched with service-impacting alerts. IT can take fast, contextually-aware action from alerts by automatically creating incidents, associating knowledge base articles, setting rules to trigger workflows, or providing automated remediation options through ServiceNow Orchestration. With integrated, service-aware Event Management, IT can proactively focus on issues that have high impact on business services and can act in a fast or preventive fashion to ensure service availability.

The screenshot displays the ServiceNow Event Management interface. At the top, there's a navigation bar with 'All' and 'Prioritize by: Business criticality'. Below this is a dashboard with several colored tiles representing different services and their health status. The tiles are color-coded: green for healthy, yellow for warning, and red for major issues. Services shown include AMEA Customer, APAC Doc, Credit, North A, EU - Customer Purch, QA Audit, UK B, UK C, UK L, APAC Account, APAC Loy, CRM, Customer Mana, North A, Production A, UK P, UKX, US A, APAC Billing, Asia Portal, Custom, Customer Purch, Order I, Production R, Retail, US Billing, User, APAC Customer, Consumer, Demographics R, exchange 2013, Prod, Purchasing T, Corp E-Ma, Custom, Edit Purchase O, and US Loyalty Cl.

Below the dashboard is an 'Alerts' section with a 'Correlated Alerts' toggle and a filter bar showing 1 alert. The table below lists the alerts:

Number	Group	Severity	Source	Description	Node	Configuration Item	Maintenance	Task	Acknowledged	Updated
Alert10012088		Major	SCDM	Exchange Service Stopped, Description: T...	V-W2K8-EX13-S2.LOCAL.LAB	y-w2k8-ex13-s2	false	false	false	02-15 11:01
Alert10012551		Minor	AppDynamics	Slow Response Time on HTTP server	V-RHEL-5-32-WEB01.localhost.localdomain	Apache	false	false	false	02-16 01:05
Alert10012553		Warning	Quest	MQ Messages Sent/Received per sec exceed...	V-W2K3-32-MQ7	WMBSQM	false	false	false	02-16 01:03
Alert10012489		Major	SCDM	Exchange Health Set, Description: The cl...	V-W2K8-EX13.LOCAL.LAB	y-w2k8-ex13	false	false	false	02-15 22:42

Service health dashboard makes it easier to identify issues and take action to eliminate service outages.

### Integration with Monitoring Tools

Event Management can integrate with multiple infrastructure-monitoring tools to receive events for processing and action. Event Management has out-of-the-box connectors to IBM NetCool, Microsoft System Center Operations Manager, HP Operations Manager, and more. For additional monitoring tools, including standalone tools for network, server, and storage management, IT can quickly integrate through a simple REST API, SNMP, or JavaScript-based custom connectors.

### Built-In and Custom Event Filters

Event Management brings in raw events and processes them to generate more qualified alerts. Built-in filters automatically evaluate various criteria to reject, normalize, and/or de-duplicate events, so the alert signal can be isolated from the event noise. ServiceNow de-duplicates events from multiple monitoring tools into a single, normalized alert. Monitored nodes correlate with ServiceNow Configuration Management Database (CMDB) configuration items (CIs), so all future events that come in on a node can relate to a CI. ServiceNow recognizes CIs in maintenance mode, suppressing any incoming events associated with those CIs. In addition, IT can create custom filters. For example, IT can filter out events from a demo source. Thus, IT can address events related to mission-critical business services, ensuring service uptime and business continuity.

### Predictive Alerts and Anomaly Detection

IT can prevent service outages by using out-of-the-box machine-learning techniques for predictive alerts and anomaly detection. The predictive alerts feature predicts knock-on effects of critical alerts, with percentage of probability, based upon historical alert patterns. By adding ServiceNow Operational Intelligence to Event Management, IT can also use operational metrics captured by monitoring tools to detect anomalies, which may indicate potential service outages. Operational metrics uses dynamically

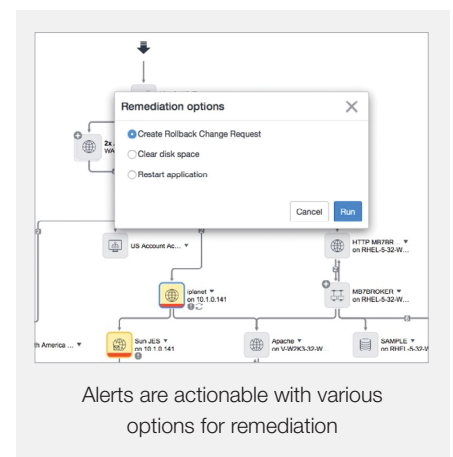
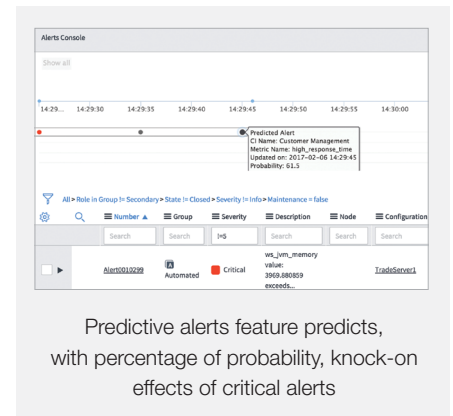
adjusted thresholds to flag out-of-band behavior of CIs, which may not be captured by events. High anomaly scores for CI attributes can indicate that a CI may be at risk to cause a service outage. Anomalies can be promoted to become alerts on the alert console and service health dashboard for preventive action.

### Consolidated Overview Dashboard

The Event Management overview dashboard provides a consolidated view of infrastructure and service health. Charts and tables in the dashboard provide an at-a-glance view of all alerts, associated incidents, top alert-generating CIs, and affected services. Current alerts, daily-digest alerts, and weekly alerts are shown in order of severity. IT can use the charts to isolate a particular machine or CI that is generating events through different monitoring tools. To view the status of all services, IT can look at an overview of alerts and their associated incidents listed by severity. This approach enables IT to prioritize incidents and take corrective action sooner. Like all ServiceNow dashboards, the visualizations are interactive and can be easily drilled into to see more details. Event Management also allows IT to do mashups of ServiceNow data, such as incidents, changes, and outages. These can be viewed from a centralized dashboard, enabling IT to see a correlation of events and tasks with data on all services and CIs—so they can identify issues quickly. In addition, the overview dashboard can be enriched with powerful insights and ad-hoc filtering provided by ServiceNow Performance Analytics.

### Service Impact View

Event Management uses ServiceNow Service Mapping to correlate alerts with services—providing a service impact view to help IT identify problems and prioritize them appropriately. Once Event Management raises an alert, the alert maps to CIs, including business services. Through an interactive service map, IT can easily see impacted CIs and their upstream and downstream dependencies.



### Automatically Actionable Alerts

Rules may be applied to alerts to facilitate faster resolution of service-impacting issues. These rules automatically trigger various actions in ServiceNow Incident Management, knowledge base, and more. IT can create a rule to auto-generate high-priority incidents for alerts based on severity and another rule to associate a knowledge base article with the high-priority incident to resolve the underlying issue. Alert rules can also trigger workflows or present automated remediation options through integration with ServiceNow Orchestration in order to restore services quickly. IT can also define SLAs for business services and CI statuses and measure the availability of business services and CIs.